January 10, 2012

E-MAIL SCAM ASKS FOR URGENT HELP AND MONEY

BISMARCK – An old e-mail scam is making the rounds again and people should be cautious, warns Attorney General Wayne Stenehjem.

The scam comes in two parts; first, the scam artist hacks into an e-mail account and then uses the hacked e-mail address to send out an "urgent" e-mail to everyone in the contact list. The e-mail, which appears to come from a friend, claims that the friend is traveling overseas and has experienced an emergency. The e-mail asks the recipient to wire money immediately so that the "friend" can return home. There are numerous variations of the scam e-mail, but they all involve an urgent request for money and a promise to repay it.

"Of course, there is no emergency. Any money that is sent goes straight into the pocket of the scam artist," said Stenehjem. "It is an unusual scam because there are two victims: the person whose e-mail account was hijacked, and the person who wired money thinking they're helping a friend," he continued.

This e-mail scam first appeared several years ago, but is being reported again across North Dakota. In the past, the scam artists used fake official looking emails to trick account holders into "confirming" account information. As consumers have become suspicious of those emails, the scam artists have moved on to more sophisticated methods, often embedding hidden viruses into e-mails that launch as soon as the e-mail or attachment is opened. As soon as the hacker has gained access to the e-mail account he changes the password, which locks out the real account owner, leaving the scam artist in control.

Stenehjem is alerting the public again after a recent Bismarck victim reported he had lost several thousand dollars because he thought a colleague was in trouble and needed the money.

Parrell Grossman, director of the Consumer Protection Division, cautions consumers to be wary of any request that directs money to be wired overseas. "Before sending any money, check to see if your friend really is traveling," he said. "Once you have wired the money, it's too late."

To help prevent an e-mail account from being hijacked, Grossman recommends that people change account passwords and security questions regularly, keep anti-virus software up to date, and run regular virus scans.

Individuals who have questions about scams or wiring money can contact the Consumer Protection division at (701) 328-3404 or toll free at 1-800-472-2600.

# # #